REMARKS

I. Introduction

In response to the Office Action dated October 6, 2003, please consider the following remarks. Re-examination and re-consideration of the application, as amended, is requested.

II. The Cited References and the Subject Invention

A. The Rallis Reference

U.S. Patent No. 6,425,084, issued July23, 2002 to Rallis et al. discloses a notebook security system using infrared key. An IR key device carries a first serial number and an encryption key. A second serial number corresponds to a device internal to the computer. A mass storage device installed in the computer stores a validation record that includes an unencrypted portion and an encrypted portion, the unencrypted portion including a copy of the first serial number and the encrypted portion including a copy of said second serial number and a user personal identification number. The key device is coupled and interfaced with an infrared port on the computer by the user. The first serial number and the encryption key are read from the key device in order to gain authorized use of the computer. The key device may be decoupled from the computer after authorized use of the computer has been gained, and during operation of the computer.

III. Office Action Prior Art Rejections

In paragraphs (1)-(2), the Office Action rejected claims 1-17 under 35 U.S.C. § 102(e) as anticipated by Rallis et al., U.S. Patent No. 6,425,084 (Rallis). Applicants respectfully traverse these rejections.

With Respect to Claims 1 and 4: Claim 1 recites an input device for securing a token from an unauthorized user. The token comprises:

> *a user interface for accepting entry of a personal identifier from a user;*
> *a processor, communicatively coupled to the user interface;*
> *a token interface, including:*
> *a token interface emitter, for producing a signal having information including the personal identifier, the token interface emitter communicatively coupled to the processor and further communicatively coupled to a token sensor when the token is physically coupled with the token interface; and*

a shield, substantially opaque to the signal, for substantially confining reception of the signal to the token sensor.

According to the Office Action, the Rallis reference discloses an input device for securing a token from an unauthorized user as follows:

> Briefly, a security system constructed in accordance with the invention implements a user-validation procedure that requires the user to connect the proper hardware "key" device to a computer at power-up to enable operation. The system can support multiple users and a single supervisor.(col. 1, lines 46-52)

The Applicants respectfully disagree. The Rallis reference discloses a system that uses a token to secure a laptop from an unauthorized user. It does not disclose an input device for securing a *token* from an unauthorized user.

The Office Action indicates that the Rallis reference teaches a user interface for accepting entry of a personal identifier from a user as follows:

> The user is prompted to connect the key device to the computer. In the preferred embodiment, the user is prompted to enter a PIN, although the system can be configured to operate without manual PIN entry. (col. 1, lines 61-65)

All the foregoing discloses only that the user can be prompted to enter a PIN. The Rallis reference teaches that this PIN is entered using the laptop computer keyboard (see claim 3, for example), not a input device having the features discussed below.

The Office Action indicates that the Rallis reference teaches a token interface comprising a token interface emitter for producing a signal having the personal identifier in FIG. 6A, and the following text:

> In an alternative interface, the IR key device 21 is equipped for Infrared (IR) communications with a notebook computer 10 via the IR port 16 as shown in FIG. 6A. Ideally, the IR key device 21 is of such shape and size as to be placed on the user's key chain. (col. 4, lines 44-48)

and

> When prompted by the user-validation program, the user aligns the IR key device 21 with the IR port 16 and depresses the switch 25 within the allotted time period (e.g. 30 seconds). The IR key device 21 transmits a message that includes the key device serial number and the encryption key using the Ultra Protocol as established by the Infrared Data Association (IrDA).(col. 4, lines 51-57)

The Rallis reference does not disclose an emitter producing a signal having the PIN entered by the user. Instead, Rallis teaches an emitter that transmits a serial number and an encryption key. The serial number and encryption key is used by a program running on the notebook computer to decrypt a validation record. The notebook computer compares the entered PIN to one stored in a decrypted validation record stored on the notebook computer, as described below.

> In Step 6, the program compares the PIN to the corresponding number stored in field 2 of the decrypted validation record. If the numbers do not match, the program moves to Step 11. If the system is configured to operate without the manual entry of a password or PIN, Steps 5 and 6 are bypassed. (col. 4, lines 15-20).

Importantly, at no time is the *PIN* transmitted anywhere.

The Office Action also alleges that the Rallis reference discloses a shield, substantially opaque to the signal, for substantially confining reception of the signal to the token sensor is disclosed as follows:

> When prompted by the user-validation program, the user aligns the IR key device 21 with the IR port 16 and depresses the switch 25 within the allotted time period (e.g. 30 seconds). The IR key device 21 transmits a message that includes the key device serial number and the encryption key using the Ultra Protocol as established by the Infrared Data Association (IrDA).(col. 4, lines 51-57)

Of course, the foregoing does not disclose a shield or any analogous structure. The Office Action therefore argues that "when the signal is transmitted, it contains a shield to assure no unauthorized interception of the signal that contains specific information (PIN, serial number, encryption key)."

It is indisputable, however, that the Rallis reference does not disclose any kind of shield, nor is any kind of signal transmitted that includes a PIN. A shield is also not inherently disclosed. Inherency "may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1269(Fed. Cir. 1991). Instead, to establish inherency, the extrinsic evidence "must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill." *Continental Can Co.,* 948 F.2d at 1268.

Because a shield is not *necessarily present* in the Rallis system, the Office Action's reliance on the inherency doctrine is misplaced, and the rejection under 35 U.S.C. § 102(e) should be withdrawn.

It is also important to note that the Rallis reference teaches away from the use of a shield, because data transmitted from the key to the notebook computer is protected by use of the "super key" access code procedure described below:

> To provide protection against the copying of the serial number and encryption key data from the key device 20, a "super key" access code procedure may be programmed by the manufacturer into the key

> device 20, and a "super key" verification step may be inserted at the start of the user validation procedure. The access code procedure requires the key device 20 to verify receipt of a matching code number before it will output the serial number and encryption key data. Preferably, the access code "hops", or changes, each time the key device 20 is accessed. (col. 4, lines 41-50)

"A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the Applicants. The degree of teaching away will of course depend on the particular facts; in general, a reference's disclosure will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the Applicants. *In re Gurley*, 27 F.3d 551, 553, 31 U.S.P.Q.2d 1130 (Fed. Cir. 1994). The Rallis reference teaches that communications between the key and the laptop computer be protected from interception by use of a matching code number. This would lead one of ordinary skill in the art down a path divergent from that which is described in the Applicants' claim 1.

For all of the reasons described above, the Applicants respectfully traverse the rejection of claim 1.

Claim 4 recites that the shield substantially circumscribes the token interface emitter. This feature is not disclosed in the Rallis reference, and therefore, claim 4 is allowable as well.

<u>With Respect to Claim 2</u>: Claim 2 recites that the token interface emitter is communicatively decoupled from the token sensor when the token is not physically coupled to the interface. According to the Office Action, this limitation is disclosed as follows:

> A flow diagram of the user-validation procedure is shown in FIG. 3. In Step 1, the user-validation program prompts the user to attach the key device 20 to the notebook computer 10. The program attempts to communicate with the key device 20 for a fixed delay period. If a key device 20 is not detected within this period, then the program proceeds to Step 11 where the computer is automatically powered down. (col. 3, lines 18-24).

The Applicants respectfully disagree. Rallis teaches a key that is communicatively coupled to the laptop computer, even when the two are not physically coupled. Hence, Rallis not only fails to disclose the features of claim 2, it teaches away from these features. Accordingly, the Applicants respectfully traverse the rejection of claim 2.

<u>With Respect to Claim 5</u>: Claim 5 recites that the token interface comprises *"a token interface sensor configured to receive the signal produced by a token emitter when the token is physically*

coupled with the token interface". According to the Office Action, this feature is described as follows.

> When prompted by the user-validation program, the user aligns the IR key device 21 with the IR port 16 and depresses the switch 25 within the allotted time period (e.g. 30 seconds). The IR key device 21 transmits a message that includes the key device serial number and the encryption key using the Ultra Protocol as established by the Infrared Data Association (IrDA).(col. 4, lines 51-57)

The Applicants respectfully disagree. The IR embodiment of the Rallis reference (the only embodiment could be interpreted to disclose a token emitter) is disclosed as an alternative embodiment, not one that is used in conjunction with the embodiment using the USB or PS/2 port. Hence, the Rallis reference fails to disclose or suggest the features recited in claim 5, and claim 5 is allowable.

<u>With Respect to Claims 6 and 7</u>: Claim 6 recites that the token emitter emits a second signal including information describing the intensity of the signal. The Office Action acknowledges that feature is not explicitly disclosed in the Rallis reference, but relying on the text reproduced below, argues "when the user has a sensor that is an IR signal, and then the signal transmits the intensity, because the sensor senses when the user is in a certain range.

> When prompted by the user-validation program, the user aligns the IR key device 21 with the IR port 16 and depresses the switch 25 within the allotted time period (e.g. 30 seconds). The IR key device 21 transmits a message that includes the key device serial number and the encryption key using the Ultra Protocol as established by the Infrared Data Association (IrDA).(col. 4, lines 51-57)

and

> In the "super key" configuration, the IR key device 21 includes both an IR transmitter and IR receiver, but does not include a transmit switch. The IR key device 21 remains the powered-down state until it receives an IR pulse. (col. 6, lines 7-10)

This, of course, does not disclose a *token emitter* (the foregoing describes an IR pulse transmitted by the laptop computer, not the key) transmitting a *second signal* having *information* describing the intensity of the (first) signal. Accordingly, the Applicants traverse the rejection of claim 6.

<u>With Respect to Claims 7</u>: Claim 7 recites that the processor controls the intensity of the first signal according to the information describing intensity of the first signal received from the second signal. The Office Action argues that this is inherently disclosed, but as described above, inherency requires more than speculation. Accordingly, the Applicants traverse the rejection of claim 7 as well.

<u>With Respect to Claim 8</u>: Claim 8 recites:

transmitting the user-entered personal identifier to the token via a communication path distinct from the USB-compliant interface.

According to the Office Action, the Rallis reference discloses the step of transmitting the user-entered personal identifier to the token via a communication path distinct from the USB-compliant interface as follows:

> When prompted by the user-validation program, the user aligns the IR key device 21 with the IR port 16 and depresses the switch 25 within the allotted time period (e.g. 30 seconds). The IR key device 21 transmits a message that includes the key device serial number and the encryption key using the Ultra Protocol as established by the Infrared Data Association (IrDA).(col. 4, lines 51-57)

Clearly, this is not the case. The Rallis reference does not disclose transmitting a PIN to the token at all, and in fact, teaches away from doing so. Accordingly, the Applicants respectfully traverse the rejection of claim 8.

With Respect to Claims 9 and 10: Claims 9 and 10 are allowable for the same reasons as claim 8.

With Respect to Claim 11: Claim 11 recites that the signal is shielded to confine reception of the signal to the sensor. This claim is allowable for the same reasons described with respect to claim 1 above.

With Respect to Claims 12-14: Claims 12 and 13 are allowable for the same reasons as claim 8.

With Respect to Claim 15: Claim 15 recites that the step of determining if the token has been accepted by the input device comprises the step of receiving a second signal produced by the token emitter after the token sensor receives a third signal in the token interface. According to the Office Action, these features are disclosed in the Rallis reference as follows:

> The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. If the first-level validation is successful, the procedure then uses the encryption key to decrypt the hard drive serial number and PIN found in the stored validation record. The procedure permits entry past the second security level only if the validation record is properly decrypted, the installed hard disk serial number matches the decrypted number, and the manually-entered PIN matches the decrypted PIN. A failure at any step in the user-validation procedure will immediately power down the computer, thereby rendering it useless to a thief not possessing the required key device.(col. 1, line 64, through col. 2, line 10).

According to the Office Action, the "third signal is the user's PIN that is incorrect." The Applicants respectfully traverse. The foregoing is completely unrelated to the subject of claim 15 (determining if the token has been accepted by the input device). Further, the user's PIN is not a signal produced by a token emitter or received by a token emitter. Accordingly, the Applicants respectfully traverse the rejection of claim 11.

With Respect to Claim 16: Claim 16 is allowable for the same reasons as claim 7.

With Respect to Claim 17: Claim 17 recites the step of *"disabling the transmission of the user-entered personal identifier until detection of the acceptance of the token to the USB port."* The Office Action indicates that these features are disclosed in Rallis as follows:

> For maximum security protection, the key device 20 is connected only during the user-validation procedure and is carried and stored separately from the notebook computer 10. (col. 2, line 67 through col. 3, lines 3)
>
> A flow diagram of the user-validation procedure is shown in FIG. 3. In Step 1, the user-validation program prompts the user to attach the key device 20 to the notebook computer 10. The program attempts to communicate with the key device 20 for a fixed delay period. If a key device 20 is not detected within this period, then the program proceeds to Step 11 where the computer is automatically powered down. (col. 3 and 18-24)

The Applicants do not understand where the foregoing passages disclose disabling the transmission of a user-entered personal identifier until detection of the acceptance of the token to the USB port. Rallis, in fact, does not teach transmitting a PIN anywhere, and certainly does not teach disabling transmission of a user-entered PIN until a token is accepted into a USB port. Accordingly, the Applicants traverse the rejection of claim 17.

IV. Dependent Claims

Dependent claims 2-7 and 9-17 incorporate the limitations of their related independent claims, and are therefore patentable on this basis. In addition, these claims recite novel elements even more remote from the cited references. Accordingly, the Applicants respectfully request that these claims be allowed as well.

V. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicants

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: January 6, 2004

By: ______________
Name: Victor G. Cooper
Reg. No.: 39,641

VGC/io